1997-09

The Network and Doctrine

Buddenberg, Rex

doctrine

The Network and Doctrine

Buddenberg/Sep97

As the discussions of 'information warfare' have progressed, there appear to be two institutions developing, separated by a yawning abyss:

At the conceptual level, we have vague, if real, notions that the information revolution has great things to offer to defense, deterrence, and warfare in general. Including major contributions to Sun T'zu's observation that the greatest battles won are those gained without fighting.

At the tactical level, we can observe commercial analogs of penetrations of computer systems over the Internet, insertion of computer viruses, theft of account/password data, intercept and eavesdrop of traffic. All of which have analogs in the tactical world of electronic warfare.

But there seems to be little strategy to connect the conceptual with the tactical. The purpose of this note is to provide the outline of such a strategy. Happily, we can again find a compelling historical parallel that spares us the need to intellectually reinvent from scratch.

Sea power strategy. This section briefly reviews the relevant portions of Mahan's sea control doctrines; as such it is no more than a review for naval officers, but may serve as a primer for those unfamiliar with the naval strategy that has driven the US Navy for the last century and the Royal Navy for the two centuries prior[1].

Some Mahan for perspective. The choice of Mahan as the parallel strategist is due to the strong analogs between the sea as an essentially neutral medium which is not siezed or owned by anyone[2]. In peacetime, the sea is a means for passage of commerce by all nations -- in effect all have command of the sea. In wartime, two strategies appear, those of sea denial and sea control. As an example, convoys provide moving havens across a more or less neutral sea, with the convoy escorts engaged in a duel with the sea denial forces, which were chiefly submarines in the two World Wars of the Industrial Age.

Sea denial. Sea denial, or commerce-destroying[3], provides a means for harrying and tiring an enemy. It may be a means to avoid losing a war. It may cause "great individual injury and discontent". But by itself, a sea denial strategy is not a war-winning one. Nor is it a particularly deterring strategy.

Sea Control. Sea control means, fundamentally, the ability to carry your, and your allies', commerce across the seas and to provide the means to project force upon a hostile, distant shore. A sea controller must limit the sea denial capabilities of the enemy. To quote the Prophet[4] again, "... when a question arises of control over distant regions, ... it must ultimately be decided by naval power, ..., which represents the communications that form so prominent a feature in all strategy."[5]

In the case of the western allies, 'distant regions' is always the case; sea control is the means to war winning.

We should note that a sea control navy is an order of magnitude more expensive than sea denial force. The emergence of Mahan's sea control strategic thinking was both a powerful intellectual driver behind acquisition of an Industrial Age Navy and an justification for it.

We should also place sea power and air power in their places: neither win wars by themselves. Rather they enable the favorable decisions on land to take place. After Trafalgar, the Royal Navy had uncontested control of the seas. This enabled the Peninsular Campaign to take place, with Wellington defeating Napoleon's generals. And the final military event was, of course, Waterloo, not a sea battle. Sea control enables the commerce -- transportation of an army to a distant theater; it doesn't do the fighting for the army.

Three illustrations place the concepts of sea control and sea denial into a reality. The first is John Paul Jones' encounter in Bonhomme Richard with HMS Serapis off the Scottish coast in 1779. Jones' mission was sea denial -- he was preying on commerce bound for England. At the tactical level, Serapis surrendered after a bloody fight -- the Americans won. At the operational level, however, the Royal Navy won -- Serapis' mission was convoy escort and her convoy made port unmolested. At the strategic level, the American purpose is being served because the requirements to escort convoys are drawing down the numbers of ships the Royal Navy can deploy to the western Atlantic theater.

In the second illustration, the Germans practiced a sea denial strategy during both world wars. The Americans and British practiced an explicit sea control strategy in the Battles of the Atlantic.

The Battle of the Atlantic in World War Two "...began from the first hour with full intensity..."[6] and was heralded by the torpedoing of *Athenia* by a U-boat. And this clearly critical battle extended until V-E day. Losing the Battle of the Atlantic would have starved Britain into submission; winning it enabled the logistics -- getting American armies into the theater. And winning it enabled power projection -- the North African and Normandy landings are good examples.

But we should note that the strategies are not mutually exclusive: in the Pacific in World War II, the US Navy practiced both strategies simultaneously. The submarine fleet was used in a sea denial role -- sinking the Japanese marus -- while the carrier battle forces and Marines were engaged in a sea control strategy.

Third, the allied air forces in the Gulf War had the initial task of gaining air superiority -- a direct analog of sea control, but in a different fluid medium. Once that objective was attained, the others could be taken in hand. The Iraqis, once the shooting started, had no control of the air and quickly lost the ability to exercise an air denial capability.

Map onto information war. The means to communicate is not 'owned' by anyone, just as the sea is not owned. In an analog world, posession of the ether for radio use is simply a ludicrous idea. Both forces can use radio and both can intercept, interfere with, spoof ... the other's use. As the Internet continues to grow and converge hitherto stovepipe technologies (like television and telephone), the notion of ownership of the Internet is fast disappearing as well. We can start to view an electronic mail envelope as the moving haven (i.e. convoy) inside of which is our protected commerce -- a message that we wish to protect from spoofing, tampering, eavesdropping, waylaying, ... Similarly many security technologies in the Internet involve 'tunneling' through the network -- setting up a secure virtual circuit for the duration of a transaction[7]. Martin Libicki gets to much the same conclusion, although without using the sea control analogy:

> *Is cyberspace, in fact, a space that can be defended -- or is it a set of largely private spaces that traffic in bytes from other largely private spaces?*[8]

Information denial. We can easily draw a parallel between sea denial and information denial. The commerce raider of the Internet is the purveyer of e-mail virii, IP address spoofs, cryptanalysis of messages.... The commerce raider is also the corrupter of router configurations and interrupter of links. All of these activities impede the flow of information across the network and all can be initiated by comparatively low-budget operations. But, like sea denial, information denial is not a war-winning strategy.

Information control:. Information control, of course, is the process of getting your traffic across the network in the face of all the information denial activities. Included in the job description are things like guaranteeing authenticity and confidentiality of traffic, ensuring the integrity of router configurations, and planning your corner of the Internet to be appropriately robust to guard against individual link outages.

Information control also entails the suppression of information denial activities.

And, again parallel to sea control, information control requires the commitment of much larger resources -- especially human capital resources -- than an information denial strategy does.

But the payoff is twofold: effective information control is a war-winning strategy -- it enables the rest of the Revolution in Military Affairs. And it is deterring -- an enemy who knows you have an information control capability is less likely to attack.

And like the Pacific experience in World War Two, information control and information denial are not mutually exclusive operations.

Summary. I believe that we can substitute information control for sea control and information denial for sea denial and come up with the same logic[9]. And just as clearly as sea control and air control are vital to Industrial Age warfighting, information control will be vital to warfare in an Information Age[10]. Execution of an Information Control strategy must be the doctrinal centerpiece of an information warfare military.

---

[1]I am using 'Mahan' in the large. His writings evolved over his tenure at the Naval War College. Further, I'd include others such as Corbett and Uhlig who have developed and added value to the basics within the label.

[2]My use of Mahan is not driven by a bias towards naval strategy per se. Rather, the sea control analogs are the most compelling. While Sun T'zu clearly is relevant to this discussion, I find that Jomini, von Clausewitz, and Douhet are simply not. Doenitz was a far better strategist than Lemay. The strategy that doesn't wash here is that occasionally embraced by the army (and incidentally, the Soviet Navy): seizing and holding territory. The information equivalent is locking up the computer -- the contents are secure, but you can't use them.

An additional note is that the current Revolution in Military Affairs lets us more finely hone a strategic dictum common to all of these military philosophers. They uniformly advise that one must concentrate ones forces, particularly for the offense. This, of course, entails the risk of providing a larger, juicier target for an enemy. We are increasingly able to concentrate firepower, or combat potential, without the requirement for concentrating forces. So the finer dictum should be to concentrate combat potential.

While I consider Douhet's theories as bankrupt, the Air Force is not without a doctrine. In fact, it is vintage Mahanian, substituting 'air control' for 'sea control'. Alas, it's too bad the Air Force can't admit it because Mahan wore the wrong color uniform.

[3]This is Mahan's term. See Mahan, A. T., The Influence of Sea Power on History: 1600-1783, Boston: Little, Brown and Co, 1896. The seminal discussion of commerce raiding is pp. 133-138. Sea denial means, of course, more than just commerce raiding. Closing of chokepoints and defensive mining fall within the denial definition.

[4] The label's not mine, but rather Secretary of War Stimson's: "But some of the Army-Navy troubles, in Stimson's view, grew from the peculiar psychology of the Navy Department, which frequently seemed to retire from the realm of logic into the dim religious world in which Neptune was God, Mahan his prophet, and the United States Navy the only true Church." Henry L. Stimson and McGeorge Bundy, On Active Service in Peace and War, New York: Harper Brothers, 1948, p. 506. This passage is quoted in Allard, Kenneth, Command, Control, and the Common Defense, National Defense University, 1996 (revised edition), p. 123 as if a common understanding of Mahan by the larger body of the Navy were a bad thing.

[5]Mahan, p. 417. This section is subtitled "Proper Disposal of the British" and is an analytical conclusion of a classical exercise in sea control.

[6]Churchill, The Gathering Storm, p.377. This is one volume of Churchill's The Second World War; my version is the Bantam printing.

[7]The Motorola Network Encryption System (NES) works in precisely this fashion as does the Unix secure shell (ssh). NES: an Internet Protocol (IP) datagram that transits from a LAN in one part of the Internet to another goes first to an NES box at the originating LAN. There it is encrypted and encapsulated inside another IP datagram which is addressed to the NES box at the the recieving LAN. That NES box removes the datagram from its encapsulating IP datagram host, decrypts it and forwards it on to the end system. An eavesdropper between to two NES boxes, sees only an IP datagram with the NES boxes' 'to' and 'from' addresses with a bunch of indecipherable bits inside. Next-generation internet technologies such as IPsec work much the same way. The analog is a (temporarily) protected sea lane such as a swept channel through a defensive minefield.

[8]Libicki, Martin, C., Defending Cyberspace and Other Metaphors, National Defense University, 1997, p.39.

[9]We needn't mindlessly invent new terminology (IW-O -- information warfare-offense, and IW-D -- defense) that have no intuitive links to sound strategic thinking.

[10]A small disclaimer is probably in order here. Just as the Industrial Age did not represent the demise of agriculture, the Information Age does not eliminate the importance of the industrial portions of our military. The need to extend man's muscles will not diminish.